

Press Releases

Ridge Creates New Division to Combat Cyber Threats

For Immediate Release
Office of the Press Secretary
June 6, 2003

The Department of Homeland Security (DHS) in implementing the President's *National Strategy to Secure Cyberspace* and the Homeland Security Act of 2002, has created the National Cyber Security Division (NCSA) under the Department's Information Analysis and Infrastructure Protection Directorate. The NCSA will provide for 24 x 7 functions, including conducting cyberspace analysis, issuing alerts and warning, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts. This Division represents a significant step toward advancing the Federal government's interaction and partnership with industry and other organizations in this critical area.

"Cyber security cuts across all aspects of critical infrastructure protection. Most businesses in this country are unable to segregate the cyber operations from the physical aspects of their business because they operate interdependently," said Secretary Ridge. "This new division will be focused on the vitally important task of protecting the nation's cyber assets so that we may best protect the nation's critical infrastructure assets."

About the National Cyber Security Division (NCSA)

The NCSA will identify, analyze and reduce cyber threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning.

The NCSA builds upon the existing capabilities transferred to DHS from the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System. The creation of the NCSA both strengthens government-wide processes for response and improves protection of critical cyber assets through maximizing and leveraging the resources of these previously separate offices. Robert Liscouski, the Assistant Secretary of Homeland Security for Infrastructure Protection, will oversee NCSA.

With 60 employees, the Division is organized around three units designed to:

- Identify risks and help reduce the vulnerabilities to government's cyber assets and coordinate with the private sector to identify and help protect America's critical cyber assets;
- Oversee a consolidated Cyber Security Tracking, Analysis, & Response Center (CSTARC), which will detect and respond to Internet events; track potential threats and vulnerabilities to cyberspace; and coordinate cyber security and incident response with federal, state, local, private sector and international partners; and
- Create, in coordination with other appropriate agencies, cyber security awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities.

Consistent with law and policy, DHS's NCSA will coordinate closely with the Office of Management and Budget and National Institute of Standards and Technology regarding the security of Federal systems and coordinate with Federal law enforcement authorities, as

appropriate. NCSO will leverage other DHS components including the Science and Technology Directorate, the U.S. Secret Service and the Department's Privacy Officer. The NCSO will work closely with the DHS Science & Technology (S&T) Directorate to implement all required programs for research and development in cyber security. While S&T will provide the actual research and development functions and execution, the NCSO will provide detailed requirements into the direction of this R&D in response to needs of our public and private sectors partners.